PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-264655
(43)Date of publication of application : 06.10.1998

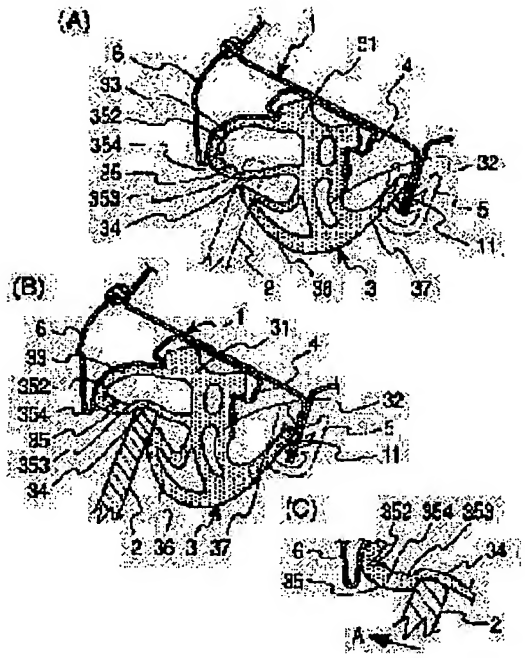
(51)Int.Cl. B60J 5/00

(21)Application number : 09-094683
(22)Date of filing : 27.03.1997

(71)Applicant : TOYODA GOSEI CO LTD
(72)Inventor : OKADA MASAYASU

(54) WEATHER STRIP FOR AUTOMOBILE

(57)Abstract:
PROBLEM TO BE SOLVED: To achieve favorable sealability around a door glass, and prevent the outward suction of the door glass in high speed run of an automobile.
SOLUTION: A curvature corner part 35 of a hollow weather strip 3 installed on a door aperture edge 1 of a car body is formed thicker than a seal wall 34, notches 352, 353 are respectively formed on an inner surface at both ends connected to a side wall 33 of the corner part 35 and the seal wall 34 to let the seal wall 34 deformed when it is pushed up by a door glass 2, and a notch 354 of a smaller groove width than the notches 352, 353 is formed at a middle position between them, so outward suction of the door glass 2 is prevented by the corner part 35 having a cross sectional surface in a gentle V-form by closing the notch 354 caught between a mould 6 provided on the door aperture edge 1 and the door glass 2.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ１）　(11)特許番号
特許第3002184号
(P3002184)
(45)発行日　平成12年１月24日(2000.1.24)　(24)登録日　平成11年11月12日(1999.11.12)

(51)Int.Cl.⁷	識別記号	FI	
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１
9/32			６７３Ｂ
			６７５Ａ

請求項の数６(全 15 頁)

(21)出願番号　特願平10－264655
(22)出願日　平成10年９月18日(1998.9.18)
審査請求日　平成10年９月18日(1998.9.18)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　庵　祥子
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　玉井　誠
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　三宅　延久
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　(外１名)
審査官　青木　重徳

最終頁に続く

(54)【発明の名称】　コンテンツ利用装置とコンテンツ利用プログラムを記録した記録媒体

1

(57)【特許請求の範囲】
【請求項１】　暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第１の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して得られる第２、第３の復号鍵を記憶する記憶手段と、
前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記記憶手段に記憶される第２の復号鍵の復号が可能かどうかを判定する判定手段と、
この判定手段で復号可能であると判定されたときには、この端末識別情報により前記暗号化された第２の復号鍵を復号化して第１の復号鍵を得、不可能であると判定されたときには、前記利用者認証情報により前記暗号化された第３の復号鍵を復号化して第１の復号鍵を得る復号手段とを有することを特徴とするコンテンツ利用装置。

2

【請求項２】　暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第１の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して得られる第２、第３の復号鍵と、任意の所定値を前記端末識別情報で暗号化して得られる暗号値とを記憶する記憶手段と、
前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記任意の所定値を暗号化し、この値と前記記憶手段に記憶される暗号値とを比較する判定手段と、
この判定手段で一致したと判定されたときには、この端末識別情報により前記暗号化された第２の復号鍵を復号化して第１の復号鍵を得、一致しないと判定されたときには、前記利用者認証情報により前記暗号化された第３

の復号鍵を復号化して第１の復号鍵を得る復号手段とを有することを特徴とするコンテンツ利用装置。

【請求項３】　前記利用者認証情報が、利用者ＩＤと利用者パスワードの組み合わせであることを特徴とする請求項１または２記載のコンテンツ利用装置。

【請求項４】　前記端末識別情報が、各端末毎に端末に付与されるＩＤであることを特徴とする請求項１または２記載のコンテンツ利用装置。

【請求項５】　暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第１の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して第２、第３の復号鍵を用意し、

前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記暗号化された第２の復号鍵の復号が可能かどうかを判定し、

復号可能であるときには、この端末識別情報により前記暗号化された第２の復号鍵を復号化して第１の復号鍵を得、

不可能であるときには、前記利用者認証情報により前記暗号化された第３の復号鍵を復号化して第１の復号鍵を得ることを特徴とするコンテンツ利用プログラムを記録した記録媒体。

【請求項６】　暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第１の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して第２、第３の復号鍵と、任意の所定値を前記端末識別情報で暗号化して得られる暗号値とを用意し、

前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記任意の所定値を暗号化し、この値と前記暗号値とを比較し、

一致したときには、この端末識別情報により前記暗号化された第２の復号鍵を復号化して第１の復号鍵を得、

一致しないときには、前記利用者認証情報により前記暗号化された第３の復号鍵を復号化して第１の復号鍵を得ることを特徴とするコンテンツ利用プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、暗号化されたデジタルコンテンツを流通・配布するのに適したコンテンツ利用装置とコンテンツ利用プログラムを記録した記録媒体に関するものである。

【０００２】

【従来の技術】近年、プログラムを含むあらゆる情報がインターネットやＣＤ－ＲＯＭなどのメディアを介して、いわゆるコンテンツとして流通・配布されるに至っている。このようなコンテンツはデジタル化され、デジタルコンテンツとしてさらに暗号化が施されて流通・配布される場合がある。

【０００３】このように暗号化したデジタルコンテンツの流通・配布に際して、暗号化したデジタルコンテンツの復号鍵を端末識別装置を用いて取り出した「端末固有番号」のみを鍵にして暗号化することが想定される。この場合には、不正使用の防止を実現し得るが、正規の利用者でもデジタルコンテンツを他の端末に複製することが不可能であるという問題がある。

【０００４】一方、暗号化したデジタルコンテンツの復号鍵を「利用者ＩＤと利用者パスワードの組み合わせ」のみを鍵にして暗号化することが想定される。この場合には、正規の利用者以外でも他端末に複製することが可能であるということ、デジタルコンテンツを利用するときには必ず利用者に「利用者ＩＤと利用者パスワードの組み合わせ」を入力させなければならないという問題がある。

【０００５】

【発明が解決しようとする課題】すなわち、暗号化されたデジタルコンテンツの流通・配布にあっては、下記に示すような解決すべき課題があった。

【０００６】１．正規の利用者が「利用者ＩＤと利用者パスワードの組み合わせ」を入力することによって他端末へデジタルコンテンツを複製することを可能にし、同時に利用者以外は他端末へのデジタルコンテンツの複製を不可能にすることによって不正使用を防止すること。

【０００７】２．暗号化されたデジタルコンテンツの復号鍵を一度でも「利用者ＩＤと利用者パスワードの組み合わせ」によって復号した場合は、それ以後復号されたときと同じ端末に格納されている限りは再び「利用者ＩＤと利用者パスワードの組み合わせ」を入力する必要をなくすこと。

【０００８】本発明は、上記課題に鑑みてなされたもので、これら課題を解決することのできるコンテンツ利用装置とコンテンツ利用プログラムを記録した記録媒体を提供することを目的とする。

【０００９】

【課題を解決するための手段】前述した目的を達成するために、本発明のうちで請求項１記載の発明は、暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第１の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して得られる第２、第３の復号鍵を記憶する記憶手段と、前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記記憶手段に記憶される第２の復号鍵の復号が可能かどうかを判定する判定手段と、この判定手段で復号可能であると判定されたときには、この端末識別情報により前記暗号化された第２の復号鍵を復

号化して第１の復号鍵を得、不可能であると判定されたときには、前記利用者認証情報により前記暗号化された第３の復号鍵を復号化して第１の復号鍵を得る復号手段とを有することを要旨とする。

【００１０】請求項１記載の本発明では、暗号化されたコンテンツの第１の復号鍵を、例えば端末識別装置を用いて取り出した利用端末の端末識別情報と、例えば利用者ＩＤと利用者パスワードの組み合わせによる利用者認証情報のそれぞれを鍵として暗号化し、第２、第３の復号鍵を得、記憶手段に記憶する。

【００１１】暗号化されたコンテンツを利用する場合は、端末識別情報か利用者認証情報のどちらかを鍵として暗号化されたコンテンツの第１の復号鍵を記憶手段に記憶される第２あるいは第３の復号鍵で復号し、コンテンツの復号を可能にする。

【００１２】また、請求項２記載の発明は、暗号化されたコンテンツと、暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第１の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して得られる第２、第３の復号鍵と、任意の所定値を前記端末識別情報で暗号化して得られる暗号値とを記憶する記憶手段と、前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記任意の所定値を暗号化し、この値と前記記憶手段に記憶される暗号値とを比較する判定手段と、この判定手段で一致したと判定されたときには、この端末識別情報により前記暗号化された第２の復号鍵を復号化して第１の復号鍵を得、一致しないと判定されたときには、前記利用者認証情報により前記暗号化された第３の復号鍵を復号化して第１の復号鍵を得る復号手段とを有することを要旨とする。

【００１３】請求項２記載の本発明では、暗号化されたコンテンツの第１の復号鍵を、端末識別装置を用いて取り出した所定の端末識別情報（端末識別番号・端末固有番号）と利用者認証情報、例えば利用者ＩＤと利用者パスワード、さらにはクレジットカード番号とその暗証番号、銀行口座番号とその暗証番号のそれぞれを適宜単独にあるいは組み合わせて鍵として暗号化する。また、暗号化されたコンテンツを利用する場合は、端末識別情報か利用者認証情報のどちらかを鍵として暗号化されたコンテンツの第１の復号鍵を復号し、コンテンツの復号を可能にする。

【００１４】正規の利用者でも他端末へ複製できないという問題は、暗号化されたコンテンツの複製を可能とし、正規の利用者が複製後初めて復号するときに利用者認証情報を入力して正規の利用者であると認証された場合のみ第１の復号鍵を復号することによって解決する。これにより、正規の利用者以外の他端末への複製を防止することができる。

【００１５】この際、入力された利用者認証情報が正しいかどうかの判定を行う。正しくない場合は、正しく第１の復号鍵を復号できない旨を伝えるエラー処理を行う。入力された利用者認証情報が正しい場合には、正しく第１の復号鍵が復号され、暗号化されたコンテンツを復号する。暗号化されたコンテンツが復号できた場合は、新たに格納された端末の端末識別番号で暗号化されたコンテンツの第１の復号鍵を再度暗号化して、以前の端末識別番号で暗号化されたコンテンツの復号鍵に上書きしておく。

【００１６】また、利用者が一度でも利用者認証情報で認証したコンテンツに対してはそれ以後、端末固有番号を利用して第１の復号鍵を復号することによって、コンテンツを利用する度に利用者認証情報を入力しなければならないという問題を解決する。

【００１７】これにより、他端末への複製に対しては、複製した暗号化されたコンテンツに対し、正規の利用者が利用者認証情報を入力することによって第１の復号鍵を復号することによって可能とし、同時に正規の利用者以外による他端末への複製を防止する。また、暗号化されたコンテンツの第１の復号鍵を一度でも利用者認証情報で復号した端末では、それ以後、端末固有番号を利用して第１の復号鍵の復号をするため利用者認証情報を入力する必要がなくなる。

【００１８】

【００１９】

【００２０】

【００２１】

【００２２】

【００２３】また、請求項３記載の発明は、前記請求項１または２記載の利用者認証情報が、利用者ＩＤと利用者パスワードの組み合わせであることを要旨とする。

【００２４】また、請求項４記載の発明は、前記請求項１または２記載の端末識別情報が、各端末毎に端末に付与されるＩＤであることを要旨とする。

【００２５】また、請求項５記載の発明は、記録媒体に、暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第１の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して第２、第３の復号鍵を用意し、前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記暗号化された第２の復号鍵の復号が可能かどうかを判定し、復号可能であるときには、この端末識別情報により前記暗号化された第２の復号鍵を復号化して第１の復号鍵を得、不可能であるときには、前記利用者認証情報により前記暗号化された第３の復号鍵を復号化して第１の復号鍵を得ることを特徴とするコンテンツ利用プログラムを記録したことを要旨とする。

【００２６】請求項５記載の本発明では、コンテンツ利

用プログラムを記録媒体として記録しているため、該記録媒体を利用して、そのコンテンツ利用プログラムの流通性を高めることができる。

【００２７】また、請求項６記載の発明は、記録媒体に、暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第１の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して第２、第３の復号鍵と、任意の所定値を前記端末識別情報で暗号化して得られる暗号値とを用意し、前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記任意の所定値を暗号化し、この値と前記暗号値とを比較し、一致したときには、この端末識別情報により前記暗号化された第２の復号鍵を復号化して第１の復号鍵を得、一致しないときには、前記利用者認証情報により前記暗号化された第３の復号鍵を復号化して第１の復号鍵を得ることを特徴とするコンテンツ利用プログラムを記録したことを要旨とする。

【００２８】請求項６記載の本発明では、コンテンツ利用プログラムを記録媒体として記録しているため、該記録媒体を利用して、そのコンテンツ利用プログラムの流通性を高めることができる。

【００２９】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【００３０】図１は本発明の一実施例の形態に係るコンテンツ利用装置を含むシステムの構成を示すブロック図である。

【００３１】図１において、１は正規利用者が使用する利用者端末であり、この利用者端末１はコンピュータネットワーク３と適宜接続することが可能であるように構成されている。また、このコンピュータネットワーク３には商店端末５が常時、接続され、さらにこのコンピュータネットワーク３には正規利用者以外の利用者端末７も適宜、接続されるものとする。

【００３２】また、本実施形態では、上記利用者端末１には、利用者認証情報取得部１１、コンテンツ取得部１３、端末識別番号取得部１５、暗号化部１７、記憶部１９、判定部２１、復号化部２３およびコンテンツ利用部２５が構成され、カードリーダ３１が内蔵され、あるいは着脱自在に接続されているものとする。

【００３３】なお、コンテンツ取得部１３には暗号化コンテンツ取得部１３ａと復号鍵取得部１３ｂが構成され、暗号化部１７には復号鍵暗号化部１７ａと所定値暗号化部１７ｂが構成され、復号化部２３には暗号化復号鍵復号化部２３ａとコンテンツ復号化部２３ｂが構成される。

【００３４】また、記憶部１９には、「暗号化した復号鍵」、「暗号化されたコンテンツ」、「利用者認証情報」、「利用者認証情報暗号化値」、「端末識別番号」および「端末識別番号暗号化値」を記憶するためのファイルが適宜設けられる。なお、通常は「利用者認証情報」と「端末識別番号」、あるいは「利用者認証情報暗号化値」と「端末識別番号暗号化値」のファイルが適宜設けられる。

【００３５】また、これら利用者認証情報取得部１１、コンテンツ取得部１３、端末識別番号取得部１５、暗号化部１７、記憶部１９、判定部２１、復号化部２３およびコンテンツ利用部２５は、通常、利用者端末１内に予め組み込まれて提供されるが、コンテンツを利用するに際して、コンテンツの流通・配布事業者から通信（無線、有線）または記録媒体を介して提供されるプログラムにより予め構築されるものであっても良い。

【００３６】以下、図１を参照して、暗号化されたデジタルコンテンツ利用装置を含むシステムの一実施形態を詳細に説明する。

【００３７】まず、端末識別番号取得部１５について説明する。

【００３８】利用者端末１の記憶部１９に、自端末を識別するための端末識別情報としての「端末識別番号」を保持する場合と、そうでない場合がある。「端末識別番号」を保持する場合には、端末識別番号取得部１５は、記憶部１９のファイル中の「端末識別番号」を取得する。一方、保持しない場合には、端末識別番号取得部１５は、ＯＳ製品番号または起動ディスクパーティションのシリアルＩＤまたは起動ディスクパーティションのボリューム名または起動ディスクパーティション容量またはこれらの情報を組み合わせた情報などを「端末識別番号」の代替として取得する。

【００３９】次に、判定部２１における処理について説明する。ここでは利用者認証情報取得部１１において、利用者認証情報、例えば利用者ＩＤと利用者パスワード、より具体的にはクレジットカード番号と銀行口座番号とそれぞれの暗証番号を単独にまたは任意の組み合わせが取得されるものとする。

【００４０】ａ）利用者認証情報、例えば利用者ＩＤと利用者パスワードをそのまま保存する場合（図２（ａ）参照）

正規の利用者の、例えば「利用者ＩＤと利用者パスワードの組み合わせ」を予め記憶部１９の「利用者認証情報」ファイルに保存しておく。そして利用者認証情報取得部１１を介して入力された「利用者ＩＤと利用者パスワードの組み合わせ」と記憶部１９に保存してある「利用者ＩＤと利用者パスワードの組み合わせ」とを判定部２１において比較し、正しいかどうかを判定し、その判定結果を音声・画面表示として出力する。

【００４１】ｂ）利用者認証情報、例えば利用者ＩＤと利用者パスワードを鍵にして所定値Ａ０を暗号化して保存する場合（図２（ｂ）参照）

暗号化部１７の所定値暗号化部１７ｂは、予め、ある任

意に設定される所定値Ａ０を正規の利用者の「利用者ＩＤと利用者パスワードの組み合わせ」を鍵として暗号化すると共に、この暗号化結果を利用者認証情報暗号化値Ａ１として記憶部１９に保存しておく。そして利用者認証情報取得部１１を介して「利用者ＩＤと利用者パスワードの組み合わせ」が入力されたときには、この「利用者ＩＤと利用者パスワードの組み合わせ」を鍵として、所定値Ａ０を暗号化する。この暗号結果をＡ２とする。判定部２１は、Ａ１とＡ２を比較し、正しいかどうかを判定し、その判定結果を音声・画面表示として出力する。

【００４２】次に、図３乃至図５を参照して、鍵ファイルを暗号化されたデジタルコンテンツのファイルに付加するタイプにおけるデジタルコンテンツ利用方法を具体的に説明する。

【００４３】図３において、ステップＳ１１で、利用者は利用者端末１を操作して、商店端末５からコンピュータネットワーク３を介して、暗号化されたデジタルコンテンツをダウンロードする。また、ダウンロードと同時に、あるいは該暗号化されたデジタルコンテンツの暗号化されていない目次もしくは見出し情報を参照して、当該デジタルコンテンツの購入を決定したときに、ステップＳ１３において暗号化されたデジタルコンテンツの復号鍵を購入する。

【００４４】そしてステップＳ１５において、購入した暗号化されたデジタルコンテンツの復号鍵を「利用者ＩＤと利用者パスワードの組み合わせ」と、利用者認証情報取得部１１を用いて取り出した利用者端末１の「端末識別番号」の２つを鍵としてそれぞれ暗号化する。この暗号化した復号鍵をステップＳ１７で暗号化されたデジタルコンテンツに付加し、それをステップＳ１９で利用者端末１に保存する。

【００４５】また、図４を参照するに、購入時の利用者端末１で暗号化されたデジタルコンテンツを復号処理して利用する際には、ステップＳ２１で「端末固有番号」を鍵にしてデジタルコンテンツの復号鍵を復号し、この復号鍵を用いてステップＳ２３で暗号化されたデジタルコンテンツを復号する。

【００４６】さらに、図５を参照するに、購入時の利用者端末以外の利用者端末７への複製は、ステップＳ３１で暗号化した復号鍵を添付した暗号化されたデジタルコンテンツを他端末に複製することによって行う。

【００４７】複製した端末で初めて暗号化されたデジタルコンテンツを利用する際は、ステップＳ３３で、利用者が「利用者ＩＤと利用者パスワードの組み合わせ」を入力する。これら利用者ＩＤおよび利用者パスワードから、判定部２１を用いて判定し（ステップＳ３５）、入力された「利用者ＩＤと利用者パスワードの組み合わせ」が正しかった場合は、ステップＳ３９に進み、暗号化されたデジタルコンテンツの復号鍵を復号し、さらにステップＳ４１で、この復号鍵を利用して、暗号化されたデジタルコンテンツを復号する。さらに、複製した端末の「端末固有番号」を鍵にして、再度復号鍵を暗号化し、暗号化されたデジタルコンテンツに添付されている以前の端末の端末固有番号を鍵にして暗号化した復号鍵に上書きする。

【００４８】一方、ステップＳ３５で、「利用者ＩＤと利用者パスワードの組み合わせ」が正しくなかった場合は、ステップＳ３７に進み、暗号化されたデジタルコンテンツが正しく復号できなかったことを伝えるエラーメッセージを返し、終了する。

【００４９】次に、図６乃至図８を参照して、鍵ファイルと暗号化されたデジタルコンテンツファイルが分離しているタイプにおけるデジタルコンテンツ利用方法を具体的に説明する。

【００５０】図６において、ステップＳ５１で、利用者は利用者端末１を操作して、商店端末５からコンピュータネットワーク３を介して、暗号化されたデジタルコンテンツをダウンロードする。また、このダウンロードと同時に、あるいは該暗号化されたデジタルコンテンツの暗号化されていない目次もしくは見出し情報を参照して、当該デジタルコンテンツの購入を決定したときに、ステップＳ５３において暗号化されたデジタルコンテンツの復号鍵を購入する。

【００５１】そしてステップＳ５５において、購入した暗号化されたデジタルコンテンツの復号鍵を「利用者ＩＤと利用者パスワードの組み合わせ」と、利用者認証情報取得部１１を用いて取り出した「利用者端末の端末識別番号」の２つを鍵として暗号化する。ステップＳ５７で、この暗号化した復号鍵をファイルとし、暗号化されたデジタルコンテンツとともに利用者端末１の記憶部１９に保存する。

【００５２】また、図７を参照するに、購入時の利用者端末１で暗号化されたデジタルコンテンツを復号処理して利用する際には、ステップＳ６１で「端末固有番号」を鍵にしてデジタルコンテンツの復号鍵を復号し、ステップＳ６３で、この復号鍵を用いて暗号化されたデジタルコンテンツを復号する。

【００５３】さらに、図８を参照するに、購入時の利用者端末以外の利用者端末７への複製は、ステップＳ７１で、暗号化されたデジタルコンテンツと２つの暗号化された復号鍵ファイルのすべてを目的の端末に複製することによって行う。

【００５４】複製した端末で初めて暗号化されたデジタルコンテンツを利用する際は、ステップＳ７３で、利用者が「利用者ＩＤと利用者パスワードの組み合わせ」を入力する。これら利用者ＩＤおよび利用者パスワードから、判定部２１を用いて判定し（ステップＳ７５）、入力された「利用者ＩＤと利用者パスワードの組み合わせ」が正しかった場合は、ステップＳ７９に進み、暗号

化されたデジタルコンテンツの復号鍵を復号し、さらにステップＳ７９で、この復号鍵を利用して、暗号化されたデジタルコンテンツを復号する。さらに、複製した端末の「端末固有番号」を鍵にして、再度復号鍵を暗号化し、以前の端末の端末固有番号を鍵にして暗号化した復号鍵ファイルに上書きする。

【００５５】一方、ステップＳ７５で、「利用者ＩＤと利用者パスワードの組み合わせ」が正しくなかった場合は、ステップＳ７７に進み、暗号化されたデジタルコンテンツが正しく復号できなかったことを伝えるエラーメッセージを返し、終了する。

【００５６】次に、図９乃至図１１を参照して、利用者ＩＤと利用者パスワードの組み合わせで暗号化した復号鍵をＩＣカードに入れるタイプにおけるデジタルコンテンツ利用方法を具体的に説明する。

【００５７】なお、ここでは図１（ｂ）に示すように利用者端末１にはカードリーダー３１が接続され、利用者がデジタルコンテンツを利用する際にはカードリーダー３１を介しての情報の入力が可能であるものとする。

【００５８】図９において、ステップＳ９１で、利用者は利用者端末１を操作して、商店端末５からコンピュータネットワーク３を介して、暗号化されたデジタルコンテンツをダウンロードする。また、このダウンロードと同時に、あるいは該暗号化されたデジタルコンテンツの暗号化されていない目次もしくは見出し情報を参照して、当該デジタルコンテンツの購入を決定したときに、ステップＳ９３において暗号化されたデジタルコンテンツの復号鍵を購入する。この購入の際には予めカードリーダー３１を利用者端末１に接続し、利用者の「利用者ＩＤ」等が記録されたＩＣカードを挿入しておく。

【００５９】そしてステップＳ９５において、購入した暗号化されたデジタルコンテンツの復号鍵を「利用者ＩＤと利用者パスワードの組み合わせ」と、利用者認証情報取得部１１を用いて取り出した「利用者端末の端末固有番号」の２つを鍵として暗号化する。

【００６０】さらに、ステップＳ９７で、この暗号化した２つの復号鍵のうち「利用者端末の端末固有番号」で暗号化した復号鍵を暗号化されたデジタルコンテンツとともに利用者端末１の記憶部１９に保存する。そして「利用者ＩＤと利用者パスワードの組み合わせ」で暗号化した復号鍵は、ステップＳ９９で、カードリーダーに挿入されているＩＣカードに保存される。

【００６１】また、図１０を参照するに、購入時の利用者端末１で暗号化されたデジタルコンテンツを利用する際には、ステップＳ１０１で「端末固有番号」を鍵にしてデジタルコンテンツの復号鍵を復号し、ステップＳ１０３で、この復号鍵を用いて暗号化されたデジタルコンテンツを復号する。

【００６２】さらに、図１１を参照するに、購入時の利用者端末以外の利用者端末７への複製は、ステップＳ１１１で、暗号化されたデジタルコンテンツのみを複製することによって行う。

【００６３】複製した端末で初めて暗号化されたデジタルコンテンツを利用する際は、ステップＳ１１３で、複製した端末にカードリーダー３１を接続して利用者のＩＣカードを挿入し、利用者が「利用者ＩＤと利用者パスワードの組み合わせ」を入力する。ステップＳ１１５において、判定部２１を用いて判定し、入力された「利用者ＩＤと利用者パスワードの組み合わせ」が正しかった場合は、ステップＳ１１９に進み、ＩＣカードに保存されている暗号化されたデジタルコンテンツの復号鍵を復号し、この復号鍵を利用して、暗号化されたデジタルコンテンツを復号する。さらに、ステップＳ１２１で、複製した端末の「端末固有番号」を鍵にして、再度復号鍵を暗号化した復号鍵ファイルを生成する。

【００６４】一方、ステップＳ１１５で、「利用者ＩＤと利用者パスワードの組み合わせ」が正しくなっかた場合は、ステップＳ１１７に進み、暗号化されたデジタルコンテンツが正しく復号できなかったことを伝えるエラーメッセージを返し、終了する。

【００６５】上述したきたように、本実施形態においては、暗号化されたデジタルコンテンツの復号鍵を、端末識別装置を用いて取り出した「端末固有番号」と「利用者ＩＤと利用者パスワードの組み合わせ」のそれぞれを鍵として暗号化する。

【００６６】また、暗号化されたデジタルコンテンツを利用する場合は、「端末識別情報」か「利用者ＩＤと利用者パスワードの組み合わせ」のどちらかを鍵として暗号化されたデジタルコンテンツの復号鍵を復号し、デジタルコンテンツの復号を可能にする。

【００６７】また、正規の利用者でも他端末へ複製できないという問題は、暗号化されたデジタルコンテンツの複製を可能とし、正規の利用者が複製後初めて復号するときに「利用者ＩＤと利用者パスワードの組み合わせ」を入力して正規の利用者であると認証された場合のみ復号することによって解決する。これにより、正規の利用者以外の他端末への複製を防止することができる。

【００６８】この際、入力された「利用者ＩＤと利用者パスワードの組み合わせ」が正しいかどうかを「利用者ＩＤおよび利用者パスワード判定装置」を用いて判定を行う。正しくない場合は、正しく復号鍵を復号できない旨を伝えるエラー処理を行う。入力された「利用者ＩＤと利用者パスワードの組み合わせ」が正しい場合には、正しく復号鍵が復号され、暗号化されたデジタルコンテンツを復号する。暗号化されたデジタルコンテンツが復号できた場合は、新たに格納された端末の端末識別番号で暗号化されたデジタルコンテンツの復号鍵を再度暗号化して、以前の端末識別番号で暗号化されたデジタルコンテンツの復号鍵に上書きしておく。

【００６９】また、利用者が一度でも「利用者ＩＤと利

用者パスワードの組み合わせ」で認証したデジタルコンテンツに対してはそれ以後「端末固有番号」を利用して復号することによって、デジタルコンテンツを利用する度に「利用者ＩＤと利用者パスワードの組み合わせ」を入力しなければならないという問題を解決する。

【００７０】前述の手段により、他端末への複製に対しては、複製した暗号化されたデジタルコンテンツに対し、正規の利用者が「利用者ＩＤと利用者パスワードの組み合わせ」を入力することによって復号鍵を復号することによって可能とし、同時に正規の利用者以外による他端末への複製を防止する。また、暗号化されたデジタルコンテンツの復号鍵を一度でも「利用者ＩＤと利用者パスワードの組み合わせ」で復号した端末では、それ以後「端末固有番号」を利用して復号鍵の復号をするため「利用者ＩＤと利用者パスワードの組み合わせ」を入力する必要がなくなる。

【００７１】なお、このようなコンテンツ利用はコンテンツ利用プログラムにより実現され、該プログラムは記録媒体に記録して提供される。

【００７２】上述してきたように、本実施形態によれば、暗号化されたデジタルコンテンツの復号鍵を、「利用者ＩＤと利用者パスワードの組み合わせ」と端末識別装置を用いて取り出した「端末固有番号」の２つを鍵として暗号化し、この２つの暗号化された復号鍵を使い分けるようにしたので、暗号化されたデジタルコンテンツ利用方法は以下の効果を持つ。

【００７３】１．「利用者ＩＤと利用者パスワードの組み合わせ」か「端末固有番号」のどちらか片方を鍵として、暗号化されたデジタルコンテンツの復号鍵を復号し、暗号化されたデジタルコンテンツの復号を可能にする。

【００７４】２．他端末へ暗号化されたデジタルコンテンツの複製を行った場合は、複製したデジタルコンテンツの初回復号時に利用者が「利用者ＩＤと利用者パスワードの組み合わせ」を入力することによってのみ可能とする。これにより正当な利用者の複製を可能とすると同時に不正使用を防止する。

【００７５】３．暗号化されたデジタルコンテンツの復号鍵を１度でも「利用者ＩＤと利用者パスワードの組み合わせ」で復号した端末では、それ以後「端末固有番号」で暗号化されたデジタルコンテンツの復号鍵で復号を行い、利用者が「利用者ＩＤと利用者パスワードの組み合わせ」を入力する手間を省くことを可能とする。

【００７６】

【発明の効果】以上説明したように、本発明は、暗号化されたコンテンツの復号鍵を、利用者認証情報と、利用端末の端末識別情報との２つを鍵としてそれぞれ暗号化し、この暗号化により得られた２つの復号鍵を使い分けるようにしたので、暗号化されたデジタルコンテンツの復号鍵を１度でも利用者認証情報で復号した端末では、それ以後、利用端末の端末識別情報で暗号化されたデジタルコンテンツの復号鍵で復号を行い、利用者が利用者認証情報を入力する手間を省くことを可能とする。

【図面の簡単な説明】

【図１】本発明に係るデジタルコンテンツ利用システムの概略の構成を示すブロック図である。

【図２】本発明の概要を明確にするためのブロック図である。

【図３】鍵ファイルをカプセルに付加するタイプにおける暗号化されたデジタルコンテンツの不正使用の防止処理手順を示すフローチャートである。

【図４】購入端末での復号処理手順を示すフローチャートである。

【図５】複製した端末での復号処理手順を示すフローチャートである。

【図６】鍵ファイルを分離するタイプにおける暗号化されたデジタルコンテンツの不正使用の防止処理手順を示すフローチャートである。

【図７】購入端末での復号処理手順を示すフローチャートである。

【図８】複製した端末での復号処理手順を示すフローチャートである。

【図９】利用者ＩＤと利用者パスワードの組み合わせで暗号化した復号鍵をＩＣカードに入れるタイプにおける暗号化されたデジタルコンテンツの不正使用の防止処理手順を示すフローチャートである。

【図１０】購入端末での復号処理手順を示すフローチャートである。

【図１１】複製した端末での復号処理手順を示すフローチャートである。

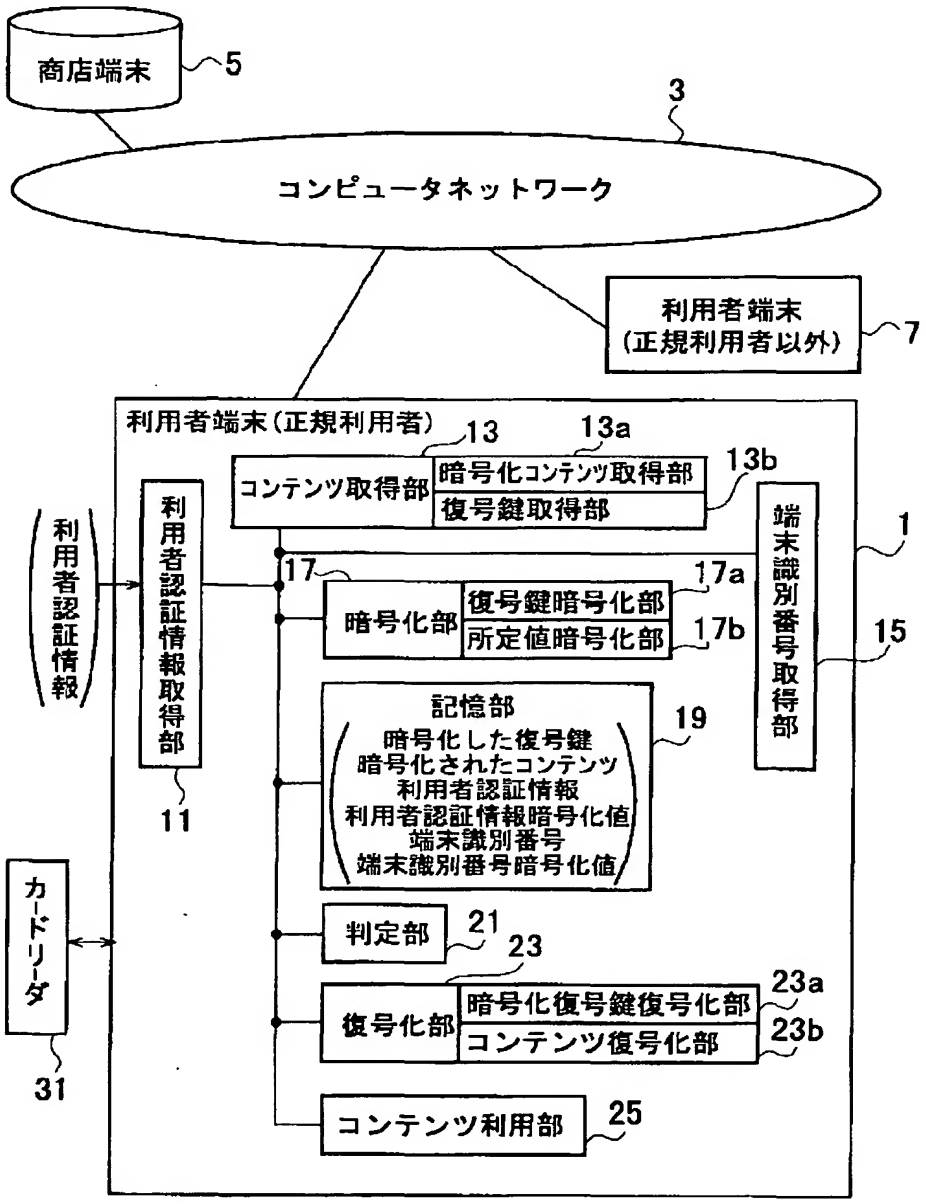
【符号の説明】

１　利用者端末（正規利用者）
３　コンピュータネットワーク
５　商店端末
７　利用者端末（正規利用者以外）
１１　利用者認証情報取得部
１３　コンテンツ取得部
１３ａ　暗号化コンテンツ取得部
１３ｂ　復号鍵取得部
１５　端末識別番号取得部
１７　暗号化部
１７ａ　復号鍵暗号化部
１７ｂ　所定値暗号化部
１９　記憶部
２１　判定部
２３　復号化部
２３ａ　暗号化復号鍵復号化部
２３ｂ　コンテンツ復号化部
２５　コンテンツ利用部
３１　カードリーダー

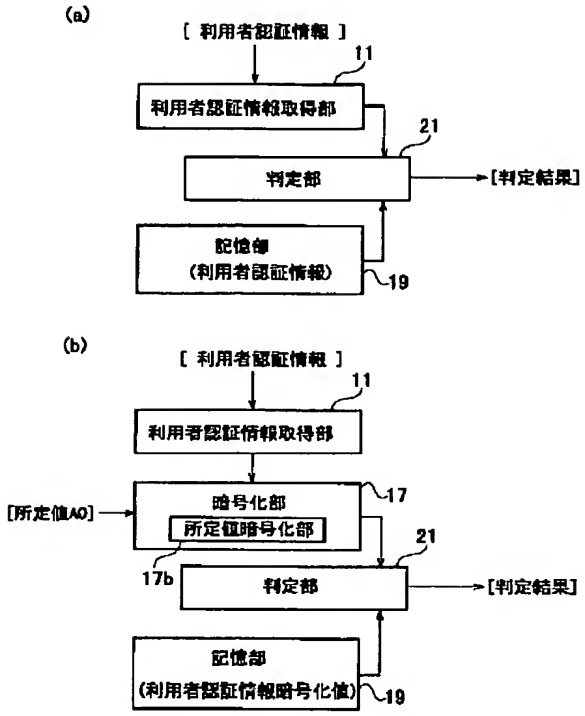
15　　16

【要約】
【課題】　本発明は、利用者が利用者認証情報を入力する手間を省くことを可能とし、正規の利用者による使用を制限することなくコンテンツの不正使用を防止することのできるコンテンツ利用方法およびその装置とコンテンツ利用プログラムを記録した記録媒体を提供することを目的とする。
【解決手段】　暗号化されたコンテンツを復号する第１の復号鍵とを取得し、所定の端末識別情報及び提供される利用者認証情報で復号鍵をそれぞれ暗号化して得られる第２、第３の復号鍵を記憶する記憶手段と、暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記記憶手段に記憶される第２の復号鍵の復号が可能かどうかを判定する判定手段で復号可能であると判定されたときには、この端末識別情報により前記暗号化された第２の復号鍵を復号化して第１の復号鍵を得、不可能であると判定されたときには、前記利用者認証情報により前記暗号化された第３の復号鍵を復号化して第１の復号鍵を得る復号手段とを備えて構成される。

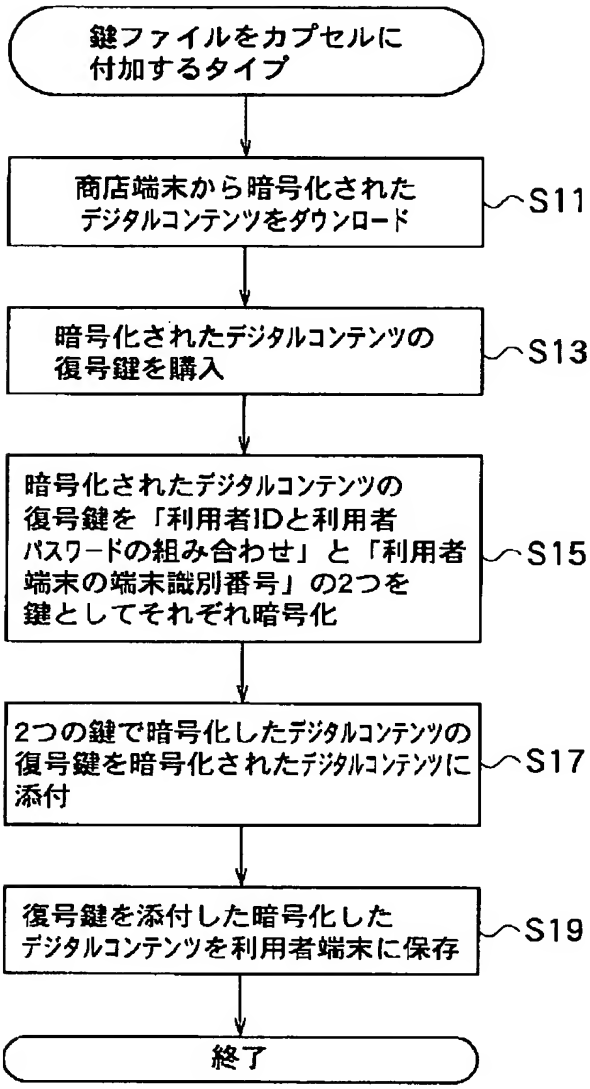
【図１】



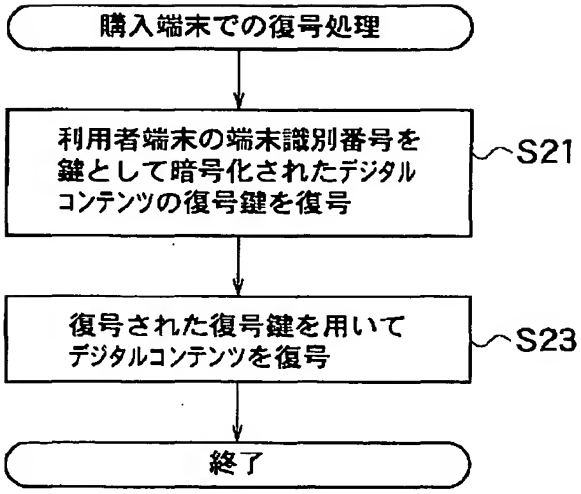
【図２】


(a)
[利用者認証情報]
11
利用者認証情報取得部
21
判定部
[判定結果]
記憶部
(利用者認証情報)
19
(b)
[利用者認証情報]
11
利用者認証情報取得部
[所定値A0]
暗号化部
所定値暗号化部
17
17b
21
判定部
[判定結果]
記憶部
(利用者認証情報暗号化値)
19

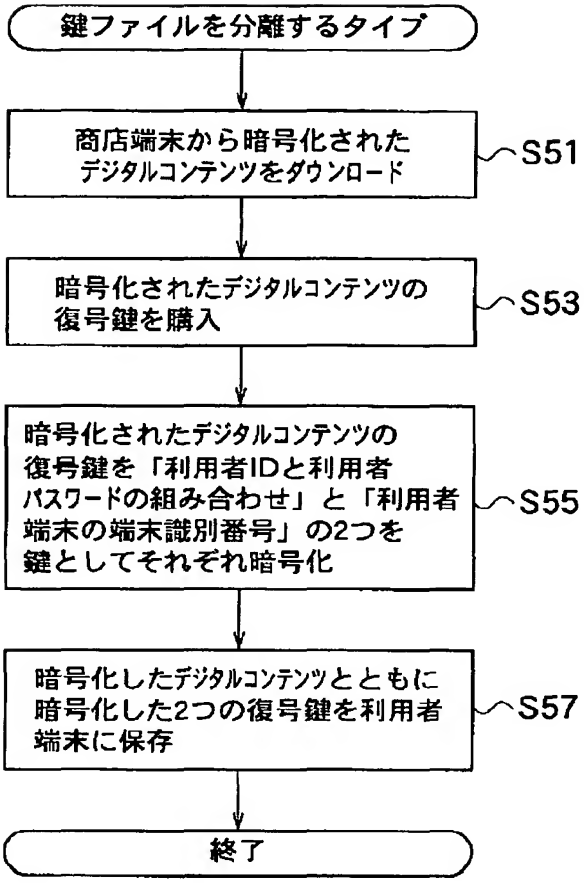
【図３】


鍵ファイルをカプセルに
付加するタイプ
商店端末から暗号化された
デジタルコンテンツをダウンロード
S11
暗号化されたデジタルコンテンツの
復号鍵を購入
S13
暗号化されたデジタルコンテンツの
復号鍵を「利用者IDと利用者
パスワードの組み合わせ」と「利用者
端末の端末識別番号」の2つを
鍵としてそれぞれ暗号化
S15
2つの鍵で暗号化したデジタルコンテンツの
復号鍵を暗号化されたデジタルコンテンツに
添付
S17
復号鍵を添付した暗号化した
デジタルコンテンツを利用者端末に保存
S19
終了

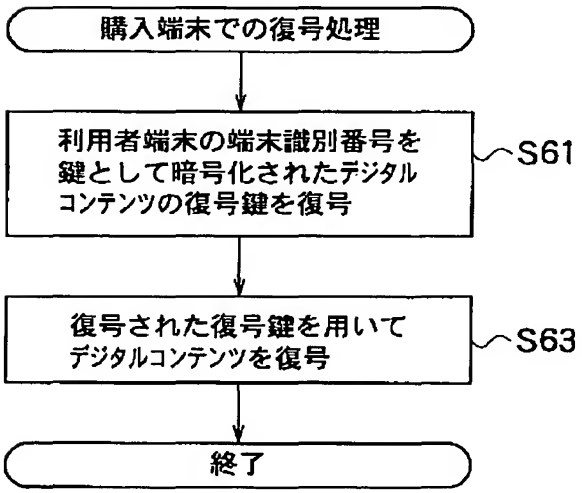
【図４】


購入端末での復号処理
利用者端末の端末識別番号を鍵として暗号化されたデジタルコンテンツの復号鍵を復号
S21
復号された復号鍵を用いてデジタルコンテンツを復号
S23
終了

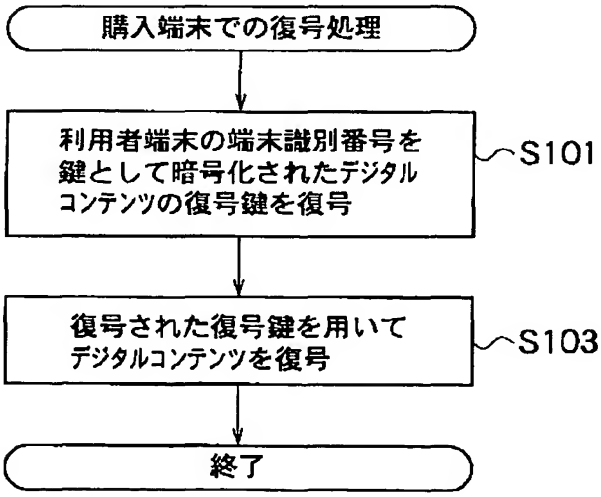
【図６】


鍵ファイルを分離するタイプ
商店端末から暗号化されたデジタルコンテンツをダウンロード
S51
暗号化されたデジタルコンテンツの復号鍵を購入
S53
暗号化されたデジタルコンテンツの復号鍵を「利用者IDと利用者パスワードの組み合わせ」と「利用者端末の端末識別番号」の2つを鍵としてそれぞれ暗号化
S55
暗号化したデジタルコンテンツとともに暗号化した2つの復号鍵を利用者端末に保存
S57
終了

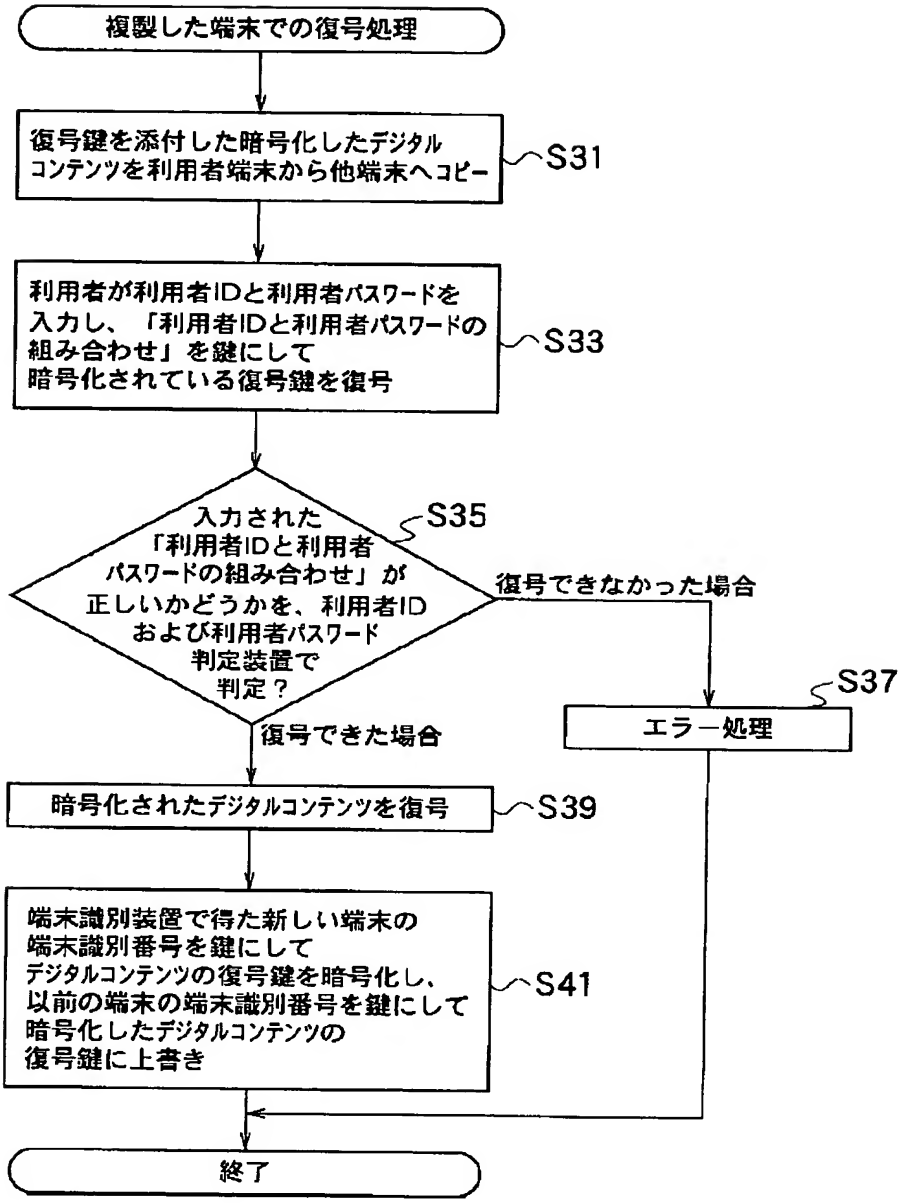
【図７】


購入端末での復号処理
利用者端末の端末識別番号を鍵として暗号化されたデジタルコンテンツの復号鍵を復号
S61
復号された復号鍵を用いてデジタルコンテンツを復号
S63
終了

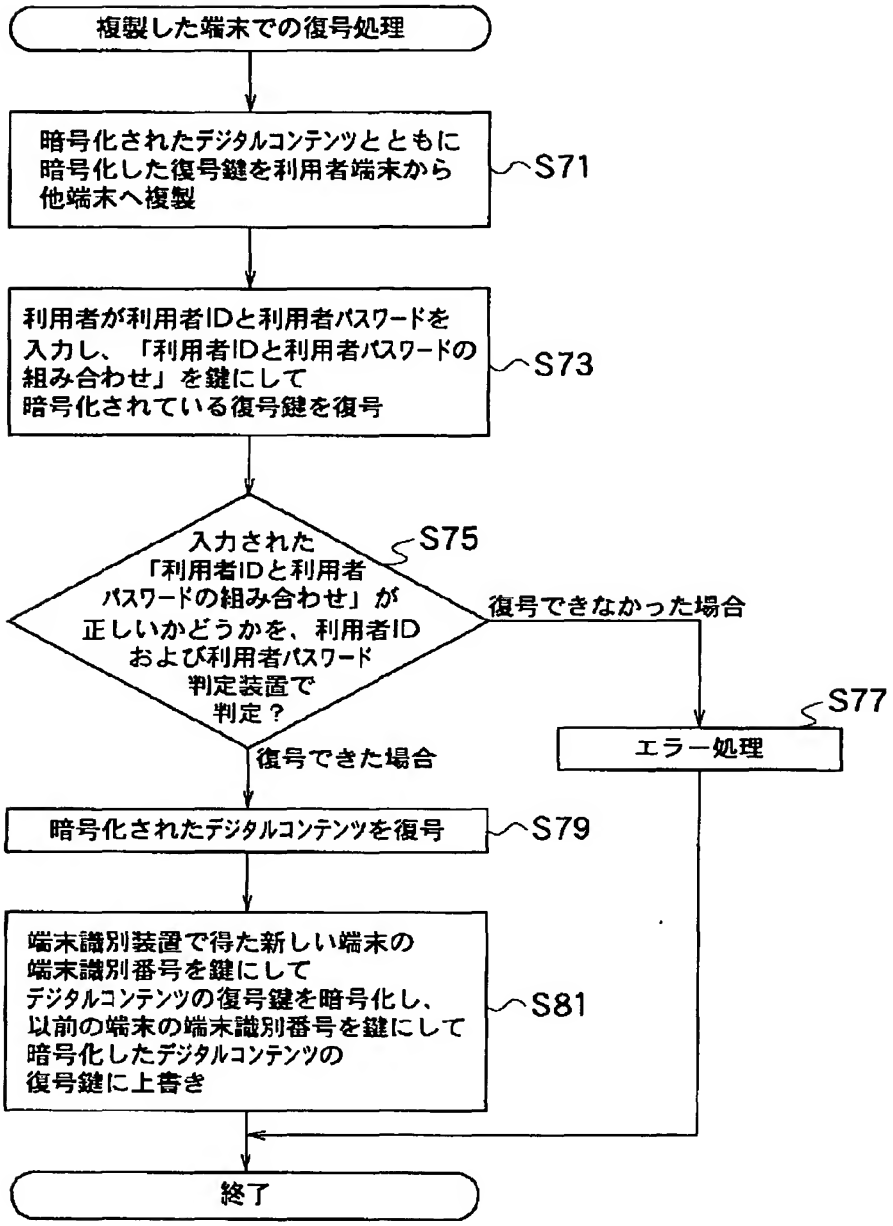
【図１０】


購入端末での復号処理
利用者端末の端末識別番号を鍵として暗号化されたデジタルコンテンツの復号鍵を復号
S101
復号された復号鍵を用いてデジタルコンテンツを復号
S103
終了

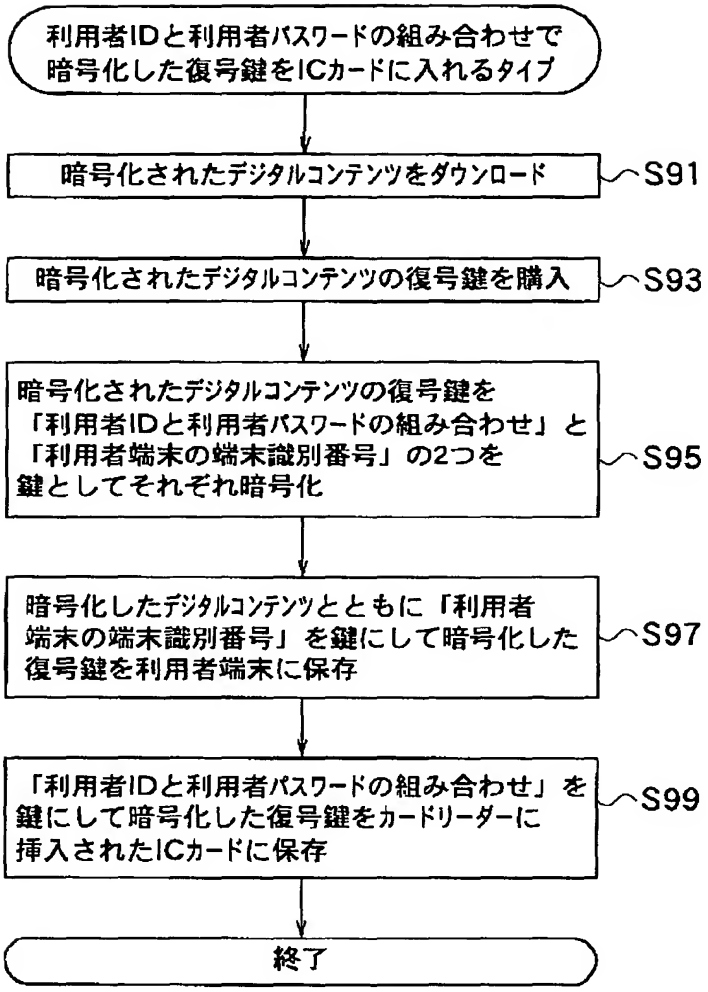
【図５】


複製した端末での復号処理
復号鍵を添付した暗号化したデジタルコンテンツを利用者端末から他端末へコピー
S31
利用者が利用者IDと利用者パスワードを入力し、「利用者IDと利用者パスワードの組み合わせ」を鍵にして暗号化されている復号鍵を復号
S33
入力された「利用者IDと利用者パスワードの組み合わせ」が正しいかどうかを、利用者IDおよび利用者パスワード判定装置で判定？
S35
復号できなかった場合
S37
エラー処理
復号できた場合
暗号化されたデジタルコンテンツを復号
S39
端末識別装置で得た新しい端末の端末識別番号を鍵にしてデジタルコンテンツの復号鍵を暗号化し、以前の端末の端末識別番号を鍵にして暗号化したデジタルコンテンツの復号鍵に上書き
S41
終了

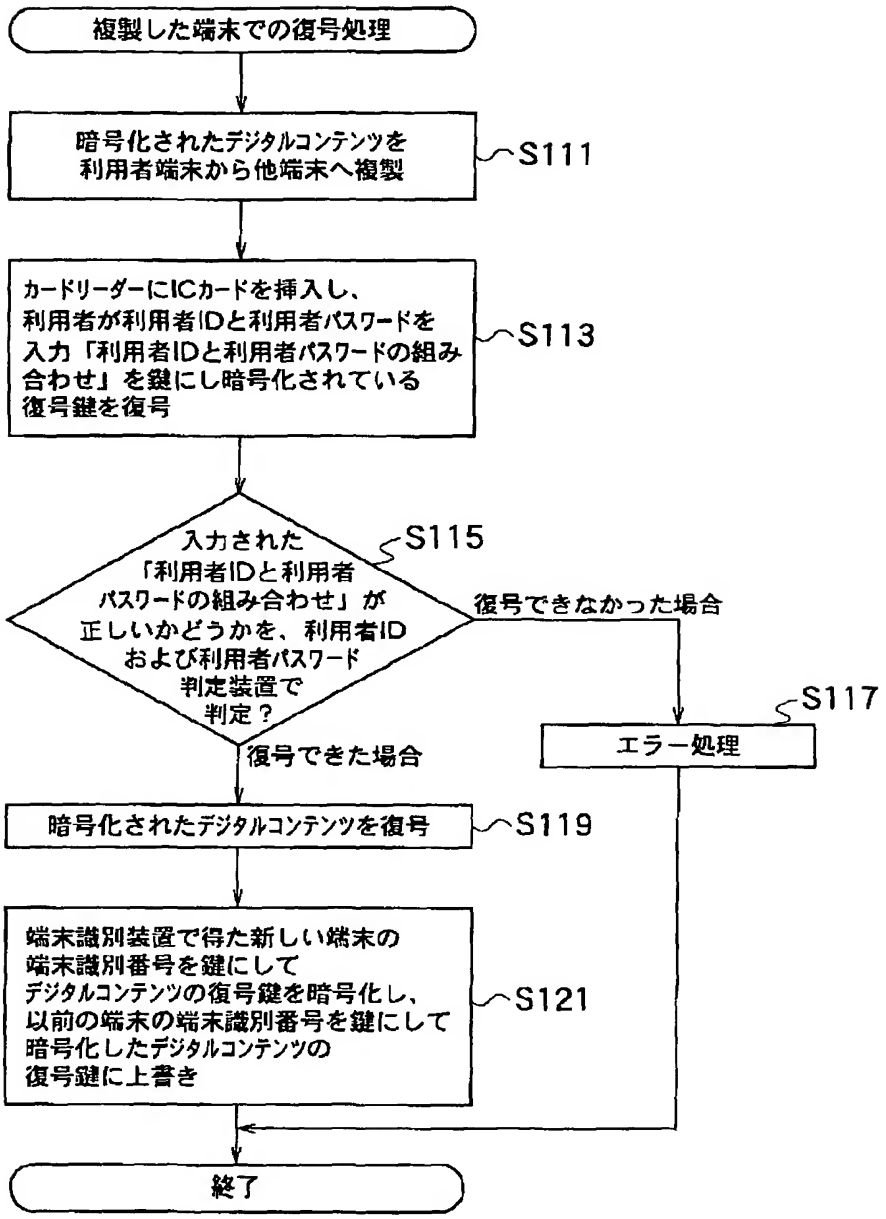
【図８】


複製した端末での復号処理
暗号化されたデジタルコンテンツとともに暗号化した復号鍵を利用者端末から他端末へ複製
S71
利用者が利用者IDと利用者パスワードを入力し、「利用者IDと利用者パスワードの組み合わせ」を鍵にして暗号化されている復号鍵を復号
S73
入力された「利用者IDと利用者パスワードの組み合わせ」が正しいかどうかを、利用者IDおよび利用者パスワード判定装置で判定？
S75
復号できなかった場合
S77
エラー処理
復号できた場合
暗号化されたデジタルコンテンツを復号
S79
端末識別装置で得た新しい端末の端末識別番号を鍵にしてデジタルコンテンツの復号鍵を暗号化し、以前の端末の端末識別番号を鍵にして暗号化したデジタルコンテンツの復号鍵に上書き
S81
終了

【図９】


利用者IDと利用者パスワードの組み合わせで暗号化した復号鍵をICカードに入れるタイプ
暗号化されたデジタルコンテンツをダウンロード
S91
暗号化されたデジタルコンテンツの復号鍵を購入
S93
暗号化されたデジタルコンテンツの復号鍵を「利用者IDと利用者パスワードの組み合わせ」と「利用者端末の端末識別番号」の2つを鍵としてそれぞれ暗号化
S95
暗号化したデジタルコンテンツとともに「利用者端末の端末識別番号」を鍵にして暗号化した復号鍵を利用者端末に保存
S97
「利用者IDと利用者パスワードの組み合わせ」を鍵にして暗号化した復号鍵をカードリーダーに挿入されたICカードに保存
S99
終了

【図１１】



フロントページの続き

(72)発明者　曽根岡　昭直
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(56)参考文献　明石　他，“インターネットを用いた情報流通プラットフォーム：ＩＮＦＯＫＥＴ－Ｉ”，ＮＴＴ　Ｒ&Ｄ，Ｖｏｌ．46，Ｎｏ．２（平９．２．10）ｐ．107－114

庵　他，“情報販売における不正コピー防止方式の提案”，情報処理学会第57回（平成10年後期）全国大会講演論文集（３）（平10．10．５）ｐ．３・23－３・24

庵　他，“不正コピー防止を考慮した情報販売方式”，情報処理学会研究報告，Ｖｏｌ．99，Ｎｏ．４（ＤＳＰ－91）ｐ．139－144

(58)調査した分野(Int.Cl.^{7}，ＤＢ名)
H04L　9/00
G09C　1/00